

Wayne Pafko  
Rhet 5112  
Prof. Wahlstrom  
Long Paper  
May 3, 2000

# Invisible Digital Watermarking: Software & Implications

## Background

Invisible digital watermarks are a new technology which could solve the “problem” of enforcing the copyright of content transmitted across shared networks. They allow a copyright holder to insert a hidden message (invisible watermark) within images, moving pictures, sound files, and even raw text. Suspicious content can be checked for the presence of the author’s watermark: “Positive detection of the [author’s] watermark...is an indication of ownership that the [author] can use as substantiated evidence in a court of law” (see Ioannis). Furthermore, the author can monitor traffic on the shared network for the presence of his or her watermark via an automated system (spider). Because this method conceals both the content of the message (cryptography) and the presence of the message (steganography) an invisible watermark is very difficult to remove. Thereby, this technology could greatly strengthen the enforcement of copyright law on the Internet.

## Overview

This paper briefly examines the practical and philosophical implications of invisible digital watermarking as applied to content on the Internet. First, we will discuss eight different shareware and freeware software packages that are currently available. Next, we will consider the practical implications of using these software packages. Finally, we will discuss some possible ethical implications of this new technology.

## Software

Eight steganographic software packages are discussed below and included on the attached CD:

### EIKONAmark v3.2

Eikmark (eikmark.zip) is a program by Alpha-Tec. It creates and detects invisible watermarks based on a unique user key (pseudorandom watermark). The software can detect the watermark even if the image’s attributes are later adjusted (color, contrast, etc.). It is designed to work with lossy compressed file formats (jpg). While the algorithm is not perfect (cropping the image can

corrupt the watermark) it does do a good job of maintaining image quality. See example below...



**Figure 1a** (castle.jpg): Original image.  
All paintings by Ted Nasmith.



**Figure 1b** (castle\_e.jpg): Watermarked image.  
Detection Key = 100001

## Gif it up v1.0

Gif it up (gif-it-up.exe) is a program by Nelsonsoft. It allows a user to hide and extract information in a gif image. However, any image modifications (crop, brightness, contrast, etc.) will corrupt the hidden information. To test the software, the following text (goblin.txt) was concealed in the image below...

Song by J.R.R. Tolkien in "The Hobbit"  
\*\*\*\*\*

Clap! Snap! the black crack!  
Grip, grab! Pinch, nab!  
And down down to Goblin-town  
You go, my lad!

Clash, crash! Crush, smash!  
Hammer and tongs! Knocker and gongs!

Pound, pound, far underground!  
Ho, ho! my lad!

Swish, smack! Whip crack!  
Batter and beat! Yammer and blast!  
Work, work! Nor dare to shirk,  
While Goblins quaff, and Goblins laugh,  
Round and round far underground  
Below, my lad!

\*\*\*\*\*



**Figure 2a** (Ride.gif): Original image.



**Figure 2b** (Ride\_e.gif): Contains hidden information (goblin.txt).

## Invisible Secrets v2.0

Invisible Secrets (invsecr2.exe) is software package from InnovaTools that allows a user to hide and encrypt data within a carrier file (jpg, bmp, or png files). Unfortunately, it is not very robust and fails when the embedded image is altered. The following text (misty.txt) was embedded in the image below:

Song by J.R.R. Tolkien in "The Hobbit"

\*\*\*\*\*

Far over the misty mountains cold  
To dungeons deep and caverns old  
We must away ere break of day  
To seek the pale enchanted gold.

The dwarves of yore made mighty spells,  
While hammers fell like ringing bells  
In places deep, where dark things sleep,  
In hollow halls beneath the fells.

For ancient king and elvish lord  
There many a gleaming golden hoard  
They shaped and wrought, and light they caught  
To hide in gems on hilt of sword.

On silver necklaces they strung  
The flowering stars, on crowns they hung  
The dragon-fire, in twisted wire  
They meshed the light of moon and sun.

Far over the misty mountains cold  
To dungeons deep and caverns old  
We must away, ere break of day,

To claim our long-forgotten gold.

Goblets they carved there for themselves  
And harps of gold; where no man delves  
There lay they long, and many a song  
Was sung unheard by men or elves.

The pines were roaring on the height,  
The winds were moaning in the night,  
The fire was red, it flaming spread;  
The trees like torches blazed with light.

The bells were ringing in the dale  
And men looked up with faces pale;  
The dragon's ire more fierce than fire  
Laid low their towers and houses frail.

The mountain smoked beneath the moon;  
The dwarves, they heard the tramp of doom.  
They fled their hall to dying fall  
Beneath his feet, beneath the moon.

Far over the misty mountains grim  
To dungeons deep and caverns dim  
We must away, ere break of day,  
To win our harps and gold from him!

\*\*\*\*\*



**Figure 3a** (mount.jpg): Original image.



**Figure 3b** (mount\_e.jpg): Contains hidden information (misty.txt). Password is 101.

## MediaSign 2000

MediaSign (mediasign-1.2demo-Win32.zip) is by MediaSec. It signs and verifies images (both lossy and other formats). Image quality is excellent. However, the algorithm is not very robust. Small changes in brightness, contrast, etc. cause it to fail to detect the watermark.



**Figure 4a** (sail.jpg): Original image.



**Figure 4b** (sail\_e.jpg): Signed image. Verify with secret key 100001.

## Snow v1.1

Snow (snwdos16.zip or snwdos32.zip) was written by Matthew Kwan. It is a program which hides information within a raw text file. It does this by adding tabs and spaces to the end of lines of text. For example, consider the following text...

-----  
A Riddle by J.R.R. Tolkien  
From "The Hobbit"

A box without hinges, key, or a lid,  
Yet golden treasure inside is hid.

-----  
**Example 3a** (riddle1.txt)

This is the raw text.

-----  
A Riddle by J.R.R. Tolkien

From "The Hobbit"

A box without hinges, key, or a lid,  
Yet golden treasure inside is hid.

-----  
**Example 3b** (hidden1.txt)

This text contains the hidden word "eggs."  
Yet the information is invisible because it is  
contained within tabs & spaces (notice the  
text wrap changed).

As this example demonstrates, this type of steganography is only useful when the data is transmitted in an unaltered format. Should someone print the encoded text (hidden1.txt) on paper and then re-digitize it, the hidden message would disappear. Furthermore, a user could delete the additional spaces and tabs in the encoded file. This would also remove the hidden information. Therefore, this type of encoding is not very robust.

## Stash v1.1.0.2

Stash (stash.zip) stores text in image files. The program was created by Smaller Animals Software. Unfortunately, encoding is limited to bmp, pxc, tif, & png formats (if converted to jpg and back the information is lost). Therefore, this encryption method is not very robust.

However, the original and encoded images appear virtually identical. Therefore, this method could be quite useful if one can guarantee that the graphic files will not be manipulated. The following text (chip.txt) was encoded in the image below:

A Song by J.R.R. Tolkien ("The Hobbit")  
\*\*\*\*\*

Chip the glasses and crack the plates!  
Blunt the knives and bend the forks!  
That's what Bilbo Baggins hates--  
Smash the bottles and burn the corks!

Cut the cloth and tread on the fat!  
Pour the milk on the pantry floor!  
Leave the bones on the bedroom mat!

Splash the wine on every door!

Dump the crocks in a boiling bowl;  
Pound them up with a thumping pole;  
And when you've finished, if any are whole,  
Send them down the hall to roll!

That's what Bilbo Baggins hates!  
So, carefully! carefully with the plates!  
\*\*\*\*\*



Figure 5a (bagend.jpg): Original image.



Figure 5b (bagend\_e.bmp): Encoded image (contains chip.txt) Method: Stash 666, 24 bit

## Steganos II Security Suite

Steganos (s2et.exe) is an excellent Steganography program by DEMCOM. It allows the user to hide information in graphic, sound, text, or HTML files. The program has a nice user interface. Unfortunately its encryption algorithm is not very robust and cannot survive lossy image compression. However, its use is not limited to images alone. It can invisibly watermark many different types of file formats. The following song (wag.txt) was hidden in the image below:

Song by J.R.R. Tolkien from "The Hobbit"  
\*\*\*\*\*

O! What are you doing,  
and where are you going?  
Your ponies need shoeing!  
The river is flowing!  
O! tra-la-la-lally  
here down in the valley!

O! What are you seeking,  
And where are you making?  
The faggots are reeking,  
The bannocks are baking!  
O! tril-lil-lil-lolly  
the valley is jolly,  
ha! ha!

O! Where are you going  
With beards all a-wagging?

No knowing, no knowing  
What brings Mister Baggins,  
And Balin and Dwalin  
down into the valley  
in June  
ha! ha!

O! Will you be staying,  
Or will you be flying?  
Your ponies are straying!  
The daylight is dying!

To fly would be folly,  
To stay would be jolly  
And listen and hark  
Till the end of the dark  
to our tune  
ha! ha!

\*\*\*\*\*



**Figure 6a** (valley.bmp): Original image.



**Figure 6b** (valley\_e.bmp): Contains hidden information (wag.txt). Unlock with password 100001.

## WinHip v1.1

WinHip (whipl1.zip) was created by Davi Tassinari de Figueiredo (a fifteen year old boy). It allows the user to hide a file inside an image. The size of the file is limited to about 1/8 the size of the image, but any type of file can be hidden. For example, a Microsoft Word file (doc) has been hidden in the image below. Even executable files could be stored this way. However, if the image is converted to a jpg (or other lossy compressed format) the hidden information is lost. Therefore this method is not very robust.



**Figure 7a** (wave.bmp): Original image.



**Figure 7b** (wave\_e.bmp): Encoded image contains a Microsoft Word file. (save as songs.doc, no password)

# Implications

In each case discussed above, a sample message was hidden-in and extracted-from a carrier file (image or text file). While some of the products were not very robust, several of the packages performed well enough that an invisible digital watermarking system could be initiated today.

Furthermore, many companies are diligently working to perfect and market this technology (see Works Cited section below). Their efforts will no doubt solve the robustness problem and any other unforeseen technical hurdles that emerge. Therefore, it is virtually ensured that invisible digital watermarking will be employed on the Internet by at least some content owners. But before we broadly adopt invisible digital watermarking we must first carefully consider the potential advantages, disadvantages, and ethical implications of using this technology.

## Advantages

- **Content Verification:** Invisible digital watermarking allows a recipient to verify the author's identity. This is important whenever falsified information could lead to costly mistakes. For example, an oil company might check for an invisible watermark in a map of oil deposits to ensure that the information is from a trusted geologic survey and not a malicious competitor. Watermarks can thus provide secure electronic signatures.
- **Determine rightful ownership:** If an author is financially damaged by unauthorized use of copyrighted material, the author is first obligated to prove rightful ownership. This can be difficult to do with digital media because of the ease with which it can be modified. Invisible digital watermarking therefore provides a secure method of proving ownership (in addition to posting a copyright notice and registering the image).
- **Track "unlawful" use:** This technology might allow an author to track how his or her content is being used. For example; automated software could scan randomly selected images on the Internet (or any digital network) and flag those images which contain the author's watermark. This covert surveillance of network traffic could rapidly detect copyright violations. It would also serve as a strong deterrent.
- **Avoid malicious removal:** The "problem" with copyright notices is that they are easy for pirates to remove. However, an invisible digital watermark is well hidden and therefore very difficult to remove. Hence, it can foil even a determined pirate's attack.

## Disadvantages

- **Degrade quality:** Even an invisible watermark will slightly alter an image during the embedding process. Therefore, they may not be appropriate for certain types of content. For example, embedding an invisible watermark in a medical scan might alter the image enough to lead to a false diagnosis.
- **May lead to "unlawful" ownership claims for images not yet watermarked:** While invisible digital watermarks are intended to reduce piracy, their widespread acceptance as a means of

legal proof of ownership may actually have the opposite effect. This is because a pirate could embed their watermark in older images not yet containing watermarks and make a malicious claim of ownership. Such claims might be difficult to challenge.

- ***No standard system in place:*** While many watermarking techniques have been proposed, none of them can yet be considered a “standard.” Furthermore, these schemes have not yet been tested in the courts. Therefore, they do not currently offer any real copyright protection.
- ***May become obsolete:*** This technology only works if the watermark resists extraction. However, technological advances might allow future pirates to remove today’s watermarks. Therefore invisible digital watermarks are somewhat unstable. An author who relies solely on invisible watermarks for copyright protection would be putting his or her content at risk of future piracy.

### Ethical Considerations

Copyright notices allow an author to claim legal ownership of an image. So too does an invisible digital watermark. They are redundant unless confronted with someone who is trying to steal an image. Therefore, it only makes sense to embed an invisible watermark if you assume that people will try to steal your image. The watermark is only useful to “catch the thief.”

However, invisible watermarks have the potential to turn a lot of innocent people into “thieves.” For example, what if a lone pirate removed the copyright notice (or added his own) and then retransmitted the image across the Internet. It would then contain a false (or non-existent) copyright notice along with the original embedded watermark. Honest individuals might subsequently use that image under a false impression of the owner’s identity (maybe they think it is in the public domain because no copyright notice remains).

In effect, our assumption that the world is full of people with malicious intent is destined to be fulfilled; even if it is largely untrue. Just because you catch someone with an illegal copy does not mean that they are actually a thief. The person may have had no idea that the image is an illegal copy, especially in an environment like the Internet where most images are automatically assumed to be in the public domain if no copyright notice is present.

So, the honest author is left with a dilemma. Is it worth the risk to use an image that appears to be in the public domain? The image may actually have an invisible digital watermark embedded—which will be detected by the author’s automated detection software—which will result in some nasty e-mails from the copyright owner—which will eventually lead to legal problems for our honest author. Therefore, it may not be worth the trouble to even use the image in the first place, even if it appears to be in the public domain.

It is hard to fault the author for this reasoning, and yet it is a sad conclusion to draw. The public might be robbed of seeing their own images (public domain images) because of the very presence of an enforced invisible digital watermarking system. Furthermore, the strict enforcement of copyright laws through watermarking techniques may give an author too much power at the public’s expense. It could be used to inhibit the “fair use” of images already provided for in the

copyright law, which states: “Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright” (excerpt from US Code TITLE 17 Sec. 107).

So, where exactly do the rights of the copyright owner end, and society’s right to use that information begin? Will invisible watermarking significantly shift the location of this boundary? Who will win and who will loss should we adopt this technology? In short, will this shift benefit or harm our society? It may in-fact do more harm than good...

## **Conclusion**

Invisible digital watermarking has rapidly advanced from theory to practice. Several of the eight shareware and freeware steganography programs examined above could be immediately used to initiate a watermarking system. Watermarking is not just a theory, it has already arrived!

However, watermarking has developed so quickly that we have not had time to adequately consider the advantages, disadvantages, and ethical implications of this technology. Do we really want this technology to become widespread? Who will benefit and who will be harmed by watermarking? Is this really in the public’s best interest?

These questions are difficult to answer because so many people do not even know that this technology exists. The only voices currently in the literature are those of the people who are creating the software or running the companies who will benefit most from this technology. Other voices and opinions need to be heard because this technology could significantly alter the relationship between content owners and the public; something in which all of us are stakeholders. This shift in power may dramatically impact the Internet, something which until now, has been a haven for the free exchange of information. It is time all of us started paying attention to this technology...

## **Works Cited**

### **Literature**

- Anderson, R., Cox, I., Low, S., Maxemchuk, N., & Tranter, W. Guest Editorial Copyright and Privacy Protection. *IEEE Journal on Selected Areas of Communications*. Vol 16, No 4. May 1998.
- Anderson, R., Fabien, A., Peticolas, P. On the Limits of Steganography. *IEEE Journal on Selected Areas in Communications*. Vol 16, NO 4. May 1998.
- Benedens, O. Geometry-Based Watermarking of 3D Models. *IEEE Computer Graphics and Applications*. Vol 19, No 1. Jan/Feb 1999.

- Busch, C., Funk, W., & Wolthusen, S. Digital Watermarking: From Concepts to Real-Time Video Applications. IEEE Computer Graphics and Applications. Vol 19, No 1. Jan/Feb 1999.
- Craver, S., Memon, N., Boon-Lock, Y., & Yeung, M. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications. IEEE Journal on Selected Areas in Communications. Vol 16, No 4. May 1998.
- Delaigle, J., De Vleeschouwer, C., & Macq, B. Watermarking Algorithm Based on a Human Visual Model. Signal Processing. Vol 66, No 3. May 1998.
- Ioannis, P. & Voyatzis, G. Protecting Digital-Image Copyrights: A Framework. IEEE Computer Graphics and Applications. Vol 19, No 1, Jan/Feb 1999.
- Low, S., Maxemchuk, N. Performance Comparison of Two Text Marking Methods. IEEE Journal on Selected Areas in Communications. Vol 16, No 4. May 1998.
- Pitas, I. & Voyatzis, G. Protecting Digital-Image Copyrights: A Framework. IEEE Computer Graphics and Applications. Vol 19, No 1. Jan/Feb 1999.
- Simmons, G. The History of Subliminal Channels. IEEE Journal on Selected Areas in Communication. Vol 16, No 4. May 1998.
- Simmons, G. Results Concerning the Bandwidth of Subliminal Channels. IEEE Journal on Selected Areas in Communications. Vol 16, No 4. May 1998.

## Web Pages

- Johnson, Neil. Steganography & Digital Watermarking. <http://www.jjtc.com/Steganography/> (visited April 3, 2000)
- Milbrandt, Eric. Watermarking Software & Companies. <http://members.tripod.com/steganography/stego/watermrk.html>. (visited April 3, 2000)
- Hartung, Frank. WWW References on Multimedia Watermarking and Data Hiding Research & Technology. <http://www-nt.e-technik.uni-erlangen.de/~hartung/watermarkinglinks.html> (visited April 3, 2000)
- Nasmith, T. (source for paintings) The Lord of The Rings. <http://www.thelordoftherings.com/> (visited April 3, 2000)

## Companies

### Alpha-Tec

- Watermarking software for images, video, and audio files.  
<http://www.alphatecltd.com/watermarking/watermarking.html>  
EIKONAmark v3.2 (eikmark.zip)  
AudioMark (audiomarkdemo.zip & audiomark.pdf)  
VidioMark (videomarkdemo.zip & videomark.pdf)

### Cognicity

- Audio watermarking  
<http://www.cognicity.com/prod/products.html>  
Audiokey

### Digimarc

Watermarking plug-ins, readers, and spiders.

<http://www.digimarc.com/imaging/software.html>

Marqspider (track copyrighted images on the web)

<http://www.digimarc.com/imaging/prspider.html>

Equitysoft

Visible watermarking

<http://www.kagi.com/equitysoft/>

H2Omarker, ImageSafe, MovieSafe, & SoundSafe.

Giovanni

Still image and audio marking.

<http://www.bluespike.com/giovanni/giovanni.html>

<http://www.bluespike.com/>

Bluespike (demo not currently available)

Mediasec

Still & multimedia markers and spiders.

<http://www.mediasec.com/products/index.html>

Mediaassign (mediasign-1.2demo-Win32.zip)

Signum Technologies

Photoshop plugin and audio marking.

<http://www.signumtech.com/suresign/index.html>

Verance Digital

Digital rights management for sound, television, & motion pictures.

<http://www.verance.com/digital/index.html>